(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
15. September 2005 (15.09.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/085992 A1

(51) Internationale Patentklassifikation[7]: G06F 7/58

(21) Internationales Aktenzeichen: PCT/EP2005/050453

(22) Internationales Anmeldedatum:
2. Februar 2005 (02.02.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 011 170.7 8. März 2004 (08.03.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: FRANKE, Andreas [DE/DE]; In der Pfeifing 36, 93138 Lappersdorf-Kareth (DE). KOLLER, Reinhold [DE/DE]; Schwarzer Helm 15, 93086 Wörth a.D. (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, 80506 München (DE).

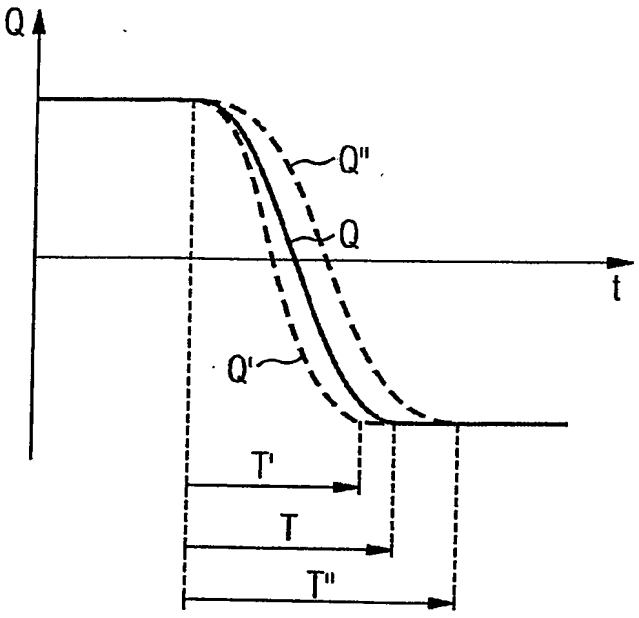
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: MANIPULATION PROOF PRODUCTION OF AUTHENTIC RANDOM NUMBERS

(54) Bezeichnung: MANIPULATIONSSICHERE ERZEUGUNG VON ECHTEN ZUFALLSZAHLEN



(57) Abstract: The invention relates to a method and device for producing an authentic random number. The inventive method consists in obtaining the authentic random number on the base of a stochastic distributed duration (t) of an electric charge exchanging process. For this purpose, the processes for exchanging charge of memory cells, for example the EEPROM or FLASH memory cells, carried out by means of a charging pump are mentioned.

(57) Zusammenfassung: Es werden ein Verfahren und eine Vorrichtung zum Erzeugen einer echten Zufallszahl vorgestellt, wobei die echte Zuffallszahl auf der Grundlage einer stochastisch verteilten Dauer (t) eines elektrischen Umladevorgangs erzeugt wird. Dabei kommen insbesondere Umladevorgänge von Speicherzellen, beispielsweise EEPROM- oder FLASH-Speicherzellen, in Betracht, die mit Hilfe einer Ladungspumpe durchgeführt werden.

WO 2005/085992 A1

GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.